創新新零售股份有限公司個人資料檔案安全維護計畫

訂定日期：中華民國114年03月31日

壹、依據：

個人資料保護法第27條第3項及數位經濟相關產業個人資料檔案安全維護管理辦法。

貳、目的：

落實個人資料檔案之安全維護及管理，防止被竊取、竄改、毀損、滅失或洩漏。

參、組織規模及特性

一、組織型態：股份有限公司

二、代表人（負責人）：李雲琴

三、公司地址：臺北市內湖區新湖一路128巷15號6樓

四、員工人數：50人以上

五、資本額：新臺幣69,019萬元

六、保有個人資料數量：約24萬筆

肆、個人資料檔案之安全維護管理措施

一、配置管理之人員及資源

（一）管理人員：

1、 配置人數：2人。

2、 職責：負責規劃、訂定、修正與執行本計畫及處理方法等相關事項，並每年向個人資料保護委員會提出報告。

（二）預算：每年新臺幣約100萬元。

二、蒐集、處理及利用個人資料之範圍及特定目的

（一）個人資料範圍界定：

1、本公司每年就本公司保有之個人資料進行清查及盤點，相關程序另訂之，附件：個資盤點表。

2、 依盤點內容，指本公司蒐集、處理及利用之自然人(包含消費者、使用者、所屬人員等)姓名、出生年月日、國民身分證統一編號、護照號碼、聯絡方式及其他得以直接或間接

方式識別該個人之資料。

（二）蒐集、處理及利用個人資料之特定目的：

行銷(040)、契約、類似契約或其他法律關係事務(069)、消費者、客戶管理與服務(090)、消費者保護(091)、網路購物及其他電子商務服務(148)、廣告或商業行為管理(152)、調查、統計與研究分析(157)。

（三）個人資料範圍含有特種個人資料（如病歷、醫療、基因、性生活、健康檢查及犯罪前科）者，應檢視是否符合個資法第6條第1項但書法定情形；個人資料範圍含有一般個人資料者，應檢視是否符合個資法第19條第1項法定情形及特定目的，經當事人同意而為蒐集或處理者，並應確保符合個資法第7條第1項規定。

（四）指定管理人員每年定期清查本公司所保有的個人資料檔案，以及其蒐集、處理和利用個人資料的作業流程，據以建立個人資料檔案清冊及個人資料作業流程說明文件。

三、個人資料之風險評估及管理機制

（一）風險評估

1、本公司每年就本公司保有之個人資料盤點內容進行風險評估，相關程序另訂之，附件：個人資料風險評估管理程序。

2、經本公司評估之高（中）風險情形如下：

(1)經由本公司或各營業處所電腦下載或外部網路入侵而外洩。

(2)經由接觸涉有個人資料之業務書件而外洩。

(3)所屬人員或第三人竊取、毀損或洩漏。

(4)與所屬單位、業間互為傳輸時外洩（包括分公司間傳輸、與相關業者間傳輸等）。

（二）管理機制

本公司每年依風險評鑑之風險結果，制訂因應風險所必要之管理措施，包含：

1、 適度設定所屬人員權限，加強使用者代碼、識別密碼之控管及妥適保管文件。

2、每季進行網路資訊安全維護及控管。

3、電子檔案資料視實際需要以加密方式傳輸。

4、加強對所屬人員及設備之管理。

四、事故之預防、通報及應變機制

（一）預防：

1、指定專人辦理安全維護事項，防止本公司保有之個人資料被竊取、竄改、毀損、滅失或洩漏。

2、本公司保有之個人資料檔案，限承辦人員使用或存取，使用或存取範圍限與其本身業務相關，且存取檔案時須鍵入其個人之使用者代碼及識別密碼。非承辦人員參閱、使用或存取相關個人資料檔案或書件時，應經負責人或經授權之管理人員同意，並留存申請授權與管理人員同意紀錄。

3、存有個人資料之儲存媒體(含可攜式媒體)，視必要性採取適當之加密機制；存有個人資料之紙本文件於不使用或下班時，遵守桌面淨空，置於抽屜或儲櫃並上鎖。

4、存有個人資料之紙本及存放媒介物於報廢汰換或轉作其他用途前，確實刪除資料或格式化，或採物理方式破壞、銷毀，並留存相關銷毀稽核紀錄。

5、電腦系統安裝防毒軟體並每季更新病毒碼，避免惡意程式與系統漏洞對作業系統之威脅。

6、對內或對外從事個人資料傳輸時，加強管控避免外洩，並留存相關紀錄。

7、加強所屬人員教育宣導，並嚴加管制並留存相關紀錄。

（二）通報及應變：

1、發現個人資料遭竊取、竄改、毀損、滅失或洩漏等安全事故時，即時向資安長通報。發生個人資料安全事故將危及正常營運或大量當事人權益者，自發現時起72小時內，以數位經濟相關產業個人資料檔案安全維護管理辦法之附表二「業者個人資料外洩通報表」通報數位發展部。

2、發生個人資料安全事故時，儘速以適當方式通知當事人事

故發生之事實、已採取之處理措施以及本公司窗口電話等資訊。窗口資訊：資安長陳宏志，電話：(02)2559-6189。

3、發生個人資料安全事故後，針對事故發生原因研議改進措施。

五、個人資料蒐集、處理及利用之內部管理措施

（一）所屬人員直接向當事人蒐集個人資料時，明確告知當事人以下事項：

1、本公司名稱。

2、蒐集目的。

3、個人資料之類別。

4、個人資料利用之期間、地區、對象及方式。

5、當事人得向本公司請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料。

6、當事人得自由選擇提供個人資料，以及如不提供對其權益之影響。

（二）所蒐集之個人資料非由當事人提供者，應於處理或利用前，向當事人告知其個人資料來源及前項應告知之事項，若當事人表示拒絕提供，應立即停止處理、利用其個人資料。

（三）利用個人資料為行銷時，當事人表示拒絕行銷後，立即停止利用其個人資料行銷，並將拒絕情形通報本公司彙整後周知所屬各部門及員工。

（四）由指定的管理人員每年清查所保有的個人資料，以確保其符合相關法定要求及特定目的。如果發現資料不再符合法定要求或超出特定目的必要範圍，或在特定目的消失、期限屆滿、契約完成履行、解除或終止後，除非法律規定、業務執行必須或經當事人書面同意，應主動刪除或銷毀該等個人資料，並留存相關紀錄。

（五）當本公司保有之個人資料利用期限屆滿時，除因法令規定、執行業務所必須或經當事人書面同意者外，將主動刪除或銷毀其個人資料，並留存相關紀錄。

（六）為維護個人資料之正確性，本公司應主動或依當事人之請求更正或補充之；當個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。因可歸責於本公司之事由，未為更正或補充之個資，應於更正或補充後，通知曾提供利用之對象。

（七）本公司委託他人或其他公司蒐集、處理或利用個人資料時，應簽訂委託契約並明確約定其內容，並於每十二個月對受託者為適當之監督。

（八）數位發展部對網際網路零售業為限制國際傳輸個人資料之命令或處分時，本公司應通知所屬人員遵循辦理。所屬人員將個人資料進行國際傳輸時，應檢視是否受數位發展部限制，並告知當事人其個人資料所欲國際傳輸之區域，且對資料接收方為下列事項之監督：

1、預定處理或利用個人資料之範圍、類別、特定目的、期間、地區、對象及方式。

2、當事人行使個資法第3條所定權利之相關事項。

六、當事人權利行使

當事人或其法定代理人向本公司表示拒絕提供，或請求閱覽、製給複製本、補充或更正、停止蒐集、處理、利用或刪除其個人資料時，採取下列方式辦理：

(一)提供聯絡窗口：創新新零售股份有限公司；及聯絡方式：(02)2559-6189，信箱：service@newretail.com.tw，相關聯絡資訊並已公告於本公司網頁。

(二)確認為個人資料當事人本人、法定代理人或經其委託之人。

(三)有個資法第10條但書、第11條第2項但書或第3項但書得拒絕當事人或其法定代理人行使權利之事由者，併附理由通知當事人或其法定代理人。

(四)遵守個資法第13條處理期限之規定。

(五)當事人查詢或請求閱覽個人資料或製給複製本者，依個資法第14條規定得酌收必要成本費用。

七、設備安全管理、資料安全管理及人員管理措施

（一）設備安全管理

1、指派專人管理建置個人資料之電腦、自動化機器相關設備、可攜式設備，應定期清點、保養維護，並應注意資料之備份及設備防竊、未經授權攜出等相關安全措施。

2、建置個人資料之個人電腦，禁止直接作為公眾查詢之前端工具。

3、應指派專人管理儲存個人資料之相關電磁紀錄物或相關媒體資料，非經單位主管同意並作成紀錄不得攜帶外出或拷貝複製。

4、電腦、自動化機器或其他存放媒介物需報廢汰換或轉作其他用途時，本公司負責人或營業處所主管應檢視該設備所儲存之個人資料是否確實刪除、銷毀。委託他人執行者，當對受託者為適當之監督並與其明確約定相關監督事項及方式。

5、更新或維修電腦設備時，應指定專人在場，確保個人資料之安全及防止個人資料外洩。

6、電腦設備報廢或不使用時，確實刪除電腦硬體設備中所儲存之個人資料檔案。

（二）資料安全管理

1、資通訊系統存取個人資料之管控：

（1）個人資料檔案存放的電腦、自動化機器相關設備或可攜式設備，應設置識別密碼、保護程式密碼、安全防護系統、加密機制及其他相關安全措施。

（2）前項安全措施應每年檢測一次，以避免或降低系統漏洞遭利用或潛在威脅。

（3）個人資料檔案使用完畢應即退出或關閉檔案，不得任其停留於電腦螢幕上。

（4）建置防火牆、電子郵件過濾機制或其他入侵偵測設備以防止外部網路入侵對策，並每月進行更新。

（5）每月進行電腦系統防毒、掃毒之必要措施，並確保系統穩定性後執行系統更新。

（6）重要個人資料應另加設管控密碼，其帳號及密碼須符合一定

之複雜度（應含英文大小寫及數字並達八碼以上）。並定期更換密碼，非經陳報本公司（商業）負責人、各營業處所主管或經指定之管理人員核可，並取得密碼者，不得存取。

（7）所屬人員非經本公司資安長核可，不得任意存取本公司保有之個人資料檔案。

（8）本公司每月對所有保有的個人資料檔案進行備份。其中屬重要個人資料者其備份應異地存放，並應建置防止個人資料遭竊取、竄改、損毀、滅失或洩漏等事故之機制。

（9）本公司蒐集、處理或利用個人資料達一萬筆以上時，設置使用者身分確認及保護機制、個人資料顯示之隱碼機制、網際網路傳輸之安全加密機制、個人資料檔案與資料庫之存取控制及保護監控措施，防止外部網路入侵對策及非法或異常使用行為之監控及因應機制。

（10）（下列擇一）

□本公司不使用真實個人資料進行資通系統測試。

□☑本公司應避免使用真實個人資料進行資通系統進行測試，若有因測試所必需而使用真實個人資料進行資通系統測試時，應遵守下列規範：取得當事人同意。

（11）本公司處理個人資料之資通系統有變更時，將確保其安全性未降低。

（12）本公司將每年檢視處理個人資料的資通系統，評估其使用狀況及存取個人資料的情形；前述檢視作業時併確認蒐集、處理或利用個人資料的電腦、相關設備或系統是否具備必要的安全性，並採取適當的安全機制。

（13）本公司將資料傳輸或儲存於AWS提供之雲端服務，並採取加密、去識別化、權限控制等適當的安全機制。

2、紙本資料之保管：

（1）本公司保有個人資料存在於紙本者，應存放於公文櫃內並上鎖，非經公司負責人、營業處所主管或經指定之管理人員同意，不得任意複製、拍攝或影印。

（2）儲存個人資料紙本之保管箱或檔案室內，應設置防火裝置及防竊措施。儲存個人資料之電腦主機系統應設置防火牆，降低外部入侵風險。主機置放之機房應設置門禁、監視錄影及防火設備。

（3）對於記載個人資料之紙本丟棄時，應先以碎紙設備進行處理。

（三）人員管理

1、依業務需求適度設定所屬人員（例如主管、非主管人員）不同之權限，以控管其個人資料蒐集、處理及利用之情形，並每十二個月檢視權限之適當性及必要性。

2、本公司所屬人員使用電腦設備蒐集、處理、利用個人資料，應以專屬帳號密碼登入電腦系統，存取個人資料檔案權限應與所職掌業務相符。專屬帳號密碼均應保密，不得洩漏或與他人共用。

3、所屬人員每年變更一次登錄電腦的識別密碼，並在變更密碼後才能繼續使用電腦。

4、所屬人員應妥善保管個人資料之儲存媒介物，執行業務時依個人資料保護法規定蒐集、處理及利用個人資料。

5、本公司與所屬人員間之勞務、承攬及委任契約均列入保密條款及相關之違約罰則，以確保其遵守對於個人資料內容之保密義務（含契約終止後）。

6、因業務需要而須利用非權限範圍之特定個人資料者，應事前提出申請，經業務主管人員同意後開放權限利用。

7、負責個人資料檔案管理人員於職務異動時，應將保管之檔案資料移交，接辦人員應另行設定密碼。

8、所屬人員離職時，應即取消其登錄電腦之使用者代碼（帳號）及識別密碼。其在職期間所持有之個人資料應確實移交，不得私自複製、留存並在外繼續利用。

八、 認知宣導及教育訓練

（一）本公司所屬人員每年計有一人參與相關單位辦理之個人資料保護法宣導或數位學習教育訓練至少三小時，以促使其明瞭個人資料

保護相關法令規定、責任範圍及應遵守之相關管理措施。前述宣導及教育訓練內容包含主管機關重要規定的宣導，如相關辦法、函釋、安維計畫等，並留存教育訓練實施紀錄，例如：簽到表、測驗結果等文件。

（二）對於負責人、管理人員應依其於本計畫所擔負之任務及角色，每年實施必要之教育訓練。

（三）對平台使用者透過本公司網頁(https://www.newretail.com.tw/)進行適當之個人資料保護及管理之認知宣導或教育訓練，並訂定個人資料保護守則，要求平台使用者遵守。

九、 個人資料安全維護稽核機制

（一）本公司每年至少乙次辦理個人資料檔案安全維護稽核，檢查本公司執行本計畫之狀況，將檢查結果作成稽核報告，並向負責人（或管理組織）提出，且經其簽名確認。

（二）針對檢查結果不符合或潛在不符合之事項，應規劃改善與預防措施，並確保相關措施之執行。執行改善與預防措施時，應依下列事項辦理：

1、確認不符合法令之內容及發生原因。

2、提出改善及預防措施方案。

3、紀錄檢查情形及結果。

十、 使用紀錄、軌跡資料及證據保存

（一）本公司執行本計畫時，應評估其必要性，保存個人資料之蒐集、處理或利用紀錄，及自動化機器設備之軌跡資料（電腦設備或其他相關之證據資料須加以保存，並製作備份保存於適當處所，以供備查)、落實執行安全維護計畫之證據，並至少留存5年。

（二）本公司建置個人資料之電腦，其個人資料使用查詢紀錄，年需將該紀錄檔備份並設定密碼，另亦將儲存該紀錄之儲存媒介物保存於適當處所以供備查。

（三）個人資料使用紀錄以紙本登記者，應存放於公文櫃內並上鎖，非經資安長核可，不得任意取出。

十一、個人資料安全維護之整體持續改善

（一）針對個資安全稽核結果不符合法令之虞者，規劃矯正與預防措施。

（二）本公司將參酌本計畫執行狀況、技術發展、業務調整及法令修正等因素，定期檢討本計畫是否合宜，必要時予以修正。

十二、業務終止後之個人資料處理方法

本公司業務終止後，所保有之個人資料不得繼續使用，並依實際情形採下列方式處理，並留存相關紀錄至少5年：

（一）銷毀：銷毀之方法、時間、地點及證明銷毀之方式。

（二）移轉：移轉之原因、對象、方法、時間、地點及受移轉對象得保有該項個人資料之合法依據。

（三）其他刪除、停止處理或利用個人資料：刪除、停止處理或利用之方法、時間或地點。